IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JOEL BELLEFEUILLE, JR., individually and on behalf of all others similarly situated, Plaintiff, v. SET FORTH, INC., Defendant.	Case No.: 1:24-cv-12188 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Joel Bellefeuille, Jr. ("Plaintiff"), on behalf of himself and all others similarly situated, by and through his undersigned counsel, brings this action against Set Forth, Inc., ("Set Forth" or "Defendant"). Plaintiff alleges as follows upon personal knowledge as to the facts pertaining to himself, and on information and belief as to all other matters.

I. SUMMARY OF THE ACTION

1. Set Forth, Inc., was founded in Illinois in 2009. Defendant provides online account administration services to consumers who are or were enrolled in debt relief programs. In the ordinary course of its business, Set Forth collected and maintained personally identifiable information of Plaintiff and putative Class Member consumers who are or are still currently its clients. The personal identifying information collected and maintained by Defendant consisted, among other things, of clients' names, addresses, and social security numbers (hereinafter sometimes referred to collectively as "PII").

2. On November 8, 2024, Set Forth disclosed, for the first time, that, on May 21, 2024, it discovered "an unauthorized user" on systems operated by Set Forth (the "Data Breach").[1] Set Forth determined that, as a result of the Data Breach, the "unauthorized user" was able to access documents containing Social Security Numbers, dates of birth, and addresses ("PII"). Set Forth now acknowledges that the PII of approximately 1.5 million consumers was exfiltrated in the Data Breach. The PII exfiltrated by cyber-criminals remains in their hands for exploitation as valuable information such cyber thieves seek and monetize.

3. Plaintiff brings this action on behalf of himself and the Nationwide Class and Sub-Class of consumers defined herein (collectively, the "Class"), the members of which (collectively, the "Class Members") had their PII, including but not limited to, names, Social Security numbers, and/or financial account information and/or other information such as phone numbers, and/or addresses, disclosed to unauthorized third persons as a result of the Data Breach.

4. Defendant is a service provider for companies that provide debt relief services. On behalf of those debt relief services, Defendant provides cloud-based account administration. As a condition of receiving cloud based debt relief program related services and account administration from Defendant, consumers provide their PII to Defendant, which it collects, receives, and maintains.

5. As part of its collecting, receiving, and maintaining the PII, Defendant represented in its "Privacy Policy" that it would safeguard the PII from unauthorized access using security measures complying with federal law, among deploying other safeguards.

6. Plaintiff and Class Members entrusted this sensitive confidential information to Defendant, which information was compromised and unlawfully accessed due to the Data Breach.

[1] https://www.setforth.com/notice-of-data-security-incident/, last visited November 25, 2024.

The information that was accessed by cyber-thieves, also remains in the possession of Defendant, despite the fact that it was accessed by unauthorized third persons, and is currently being maintained without appropriate and necessary safeguards, independent review, and oversight, and therefore remains vulnerable to additional hackers and theft.

7. The Data Breach was a direct result of Defendant's failure to implement adequate and cyber-security procedures and protocols necessary to protect Plaintiff and Class Members' PII. The Data Breach occurred because Defendant maintained Class Members' PII in a reckless manner and on its computer networks in a condition that was vulnerable to cyber-attacks.

8. The risk of cyber-attack was well-known to Defendant – and to all financial service companies. Defendant was continuously on notice at all times material that its failure to take steps necessary to secure the PII from a risk of cyber-attack and unauthorized access left that information and property in a dangerous condition that was vulnerable to theft. Defendant's failure to protect the PII of consumers is all the more egregious because it was aware of the significant risk of cyber-attacks faced by financial institutions given the sensitive nature of the PII entrusted to them.

9. Nevertheless, and despite this knowledge and recent exposure to a data breach, Defendant continuously disregarded the rights of Plaintiff and Class Members, as more fully defined below, by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its data systems were protected and safeguarded against unauthorized intrusions, while failing to disclose that it did not have adequately robust computer systems and security safeguards or practices in place with respect to protecting against the risk of unauthorized access of PII. Defendant further failed to take standard and reasonably available steps to prevent the Data Breach, and failed to properly train its staff and employees on proper security measures.

10. Importantly, Defendant also failed to provide Plaintiff and Class Members with prompt and timely notice of the Data Breach, thereby further injuring them by such delay. Defendant and its employees failed to properly monitor the computer networking systems on which it housed the PII and, had they done so, would have discovered the intrusion sooner, and would not have otherwise permitted cyber thieves to freely access Set Forth platform and network for a substantial duration of time.

11. The PII that was collected by the Defendant and maintained at all times material, without adequate safeguards, is now in the hands of cyber thieves – a present risk that will continue throughout their respective life-times as a consequence of Defendant's misconduct.

12. Defendant was fully aware at all times material that data thieves, once armed with PII that they accessed in a data breach, are capable of pursuing numerous types of misconduct and crimes through the unauthorized use and exploitation of that data, including opening new financial accounts in Class Member's names, taking loans in their names, using their names to obtain medical services, obtain government benefits, file fraudulent tax returns in order to get refunds to which they are not even entitled, and numerous other assorted acts of thievery and fraud.

13. Plaintiff and Class Members have suffered actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damages to and

diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their PII against theft and not allow access to and misuse of their personal data by others; and (h) the continued risk to their PII remaining in the possession of Defendant, and is subject to further injurious breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members' PII, and, at the very least, are entitled to nominal damages.

14. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals who are Class Members, and further seeks remedies that include, but are not limited to, compensatory damages, nominal damages and reimbursement of out-of-pocket costs, as well as injunctive and equitable relief to prevent future injury on behalf of themselves and the putative class.

II. PARTIES

Plaintiff

15. Plaintiff Joel Bellefeuille, Jr. ("Bellefeuille") is, and at all relevant times was, a resident of Holland, Michigan. Plaintiff Bellefeuille used the Set Forth software platform in relation to account he held with Freedom Debt Relief and Cordoba Legal Group. As an account administrator for Plaintiff, Set Forth was provided with critical PII, including Plaintiff's name, address, and Social Security Number.

16. On or about November 8, 2024, Plaintiff Bellefeuille received a letter from Defendant notifying of the Data Breach and stating that his PII was his PII was included in the Data Breach.

17. Plaintiff remains concerned about the fact that the Data Breach has exposed his PII to a lifetime of fraud risk. Plaintiff takes care to protect his PII from disclosure.

18. Subsequent to the Data Breach Plaintiff Bellefeuille has experienced attempted fraud. In September 2024, Plaintiff Bellefeuille noticed a fraudulent charge for $34.55 on his debit card. While this charge was subsequently reversed, Plaintiff Bellefeuille spent time addressing this charge that would have been unnecessary, but for the Data Breach. In addition, Plaintiff Bellefeuille must continue to be on guard for signs of fraud or identity theft.

19. Since receiving notice of the Data Breach, Plaintiff has taken steps to protect himself against identity theft. Plaintiff has spent time monitoring his financial accounts for signs of fraud or misuse of his PII, time that Plaintiff would not have had to expend were it not for the Data Breach.

Defendant

20. Defendant Set Forth, Inc., is a corporation incorporated in Delaware and with its principal place of business at 1900 E Golf Road, Suite 550, Schaumburg, Illinois 60173.

III. JURISDICTION AND VENUE

21. This Court has original jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because the matter in controversy, exclusive of interest and costs, exceeds the sum value of $5,000,000.00, consists of putative class membership of greater than 100 members, and is a class action in which some of the members of the Class, are citizens of states different than that of Defendant.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant is authorized to conduct business within this District, is headquartered in this District, has intentionally availed itself of the laws in this District, and conducts substantial business, including acts underlying the allegations of this complaint, in this District.

IV. FACTUAL ALLEGATIONS

Defendant's Collecting and Storing of the PII of Plaintiff and the Class and Its Related Privacy Policy

23. Defendant describes itself as "a dedicated account administrator and processor for consumers enrolled in a debt relief program" that "ensure[s] consumers' funds are in their control and held securely throughout the program."[2]

24. Defendant holds itself out as conducting "cloud-based customer relationship management (CRM) solutions powered by the Set Forth platform."[3] At all times material, and as a fundamental part of its business, Defendant collects, receives, and maintain the PII of hundreds of thousands of its current and former consumers.

25. Set Forth collected, stored, and maintained the PII provided by Plaintiff and Class Members as a condition of providing services. Such PII included Social Security Numbers, dates of birth, and addresses.

26. In order to obtain Set Forth's debt relief program services, Plaintiff and Class Members were required to and did in fact turn over such PII to Defendant.

27. Upon collecting the PII, Defendant agreed it would maintain and safeguard such data in accordance with its internal policies, state law, and federal law.

28. In that regard, Defendant was under a duty to protect its current and former consumers' PII and to timely notify them about breaches.

---

[2] https://www.setforth.com/consumers/, last visited November 25, 2024.

[3] *Notice of Data Security Incident*, FORTH, https://www.setforth.com/notice-of-data-securityincident/ (last visited Nov. 19, 2024).

29. Defendant's "Privacy Policy" boasted, represented, and assured that:

a. "Forth, Inc. (hereinafter 'Forth™' or 'Forth') is dedicated to protecting your privacy and providing you with the highest level of service."[4]

b. "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law."[5]

c. "These measures include computer safeguards and secured files and buildings."[6]

d. "We also attempt to limit personal information access to only employees, agents and representatives who need to know.[7]

30. Defendant was aware, at all times material, of the fact that as a company in the financial industry it was at risk of a cyber-security attack and data breach as many have occurred in recent years throughout the United States. Given its maintenance of critical PII, and its knowledge of such risk and its duties, Defendant was continuously responsible at all times material, for safeguarding the PII in its possession with respect to each Plaintiff and Class Member.

[4] *Privacy Policy*, FORTH, https://www.setforth.com/privacy-policy/ (last visited Nov. 19, 2024).
[5] *Id.*
[6] *Privacy Policy*, FORTH, https://www.setforth.com/privacy-policy/ (last visited Nov. 19, 2024).
[7] *Id.*

The Untimely Disclosed Cyber-Attack and Data Breach

31. In a Notice of Data Breach[8] letter dated on or about November 8, 2024 (the "Notice Letter"), Set Forth acknowledged a massive breach that began no later than May 21, 2024, informing consumers that:[9]

> **What Happened?**
>
> On May 21, 2024, Forth identified suspicious activity on its system, and immediately implemented our incident response protocols, and engaged independent computer forensic specialists to investigate the activity and determine what, if any, data may have been impacted. The investigation determined that personal information belonging to yourself, a spouse, co-applicant, or dependent may have been accessed during the incident. While there is no evidence to suggest that your information has been misused, we wanted to make you aware of this incident out of an abundance of caution.
>
> **What Information Was Involved?**
>
> From our review, it appears that your name, address, date of birth, and social security number may have been affected.

Upon information and belief, the cyber-attack and theft injured at least 1,500,000 persons, which include Defendant's current and former consumers.[10]

32. Defendant's negligence and resulting inadequate security is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII. Consequently, Defendant caused widespread injury and monetary damages.

---

[8] *Notice of Data Security Incident*, FOURTH, https://www.setforth.com/notice-of-data-security-incident/ (last visited November 25, 2024).

[9] The Notice Letter. A sample copy is available at https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792a1252b4f8318/5c00fedb-134a-4436-b778-5df30b84cdab.html

[10] *Data Breach Notifications*, MAINE ATTY GEN, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792a1252b4f8318/5c00fedb-134a-4436-b778-5df30b84cdab.html (last visited Nov. 19, 2024), *see also Notice of Data Security Incident,* FORTH, https://www.setforth.com/notice-of-data-securityincident/ (last visited Nov. 19, 2024).

33. While Defendant has offered some victims credit monitoring and identity related services upon information and belief, such services are wholly insufficient to compensate Plaintiff and Class Members for the injuries that Defendant inflicted upon them.

34. Because of the Data Breach, the sensitive PII of Plaintiff and Class Members was placed into the hands of cybercriminals— causing them injury and significant damages.

35. According to the Harvard Business Review "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."

36. Upon information and belief, Plaintiff and the Class's stolen PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

37. Plaintiff are informed and believe that the cyber-attack targeted Defendant by reason of its status as a financial institution that collects, creates, and maintains PII, and that such attack was designed to gain access to and infiltrate private and confidential data, including the PII of Plaintiff and Class Members.

Data Breaches and the Market for PII

38. Data breaches in the United States have become ubiquitous, with the goal of criminals being to monetize the stolen data.[11]

[11] Ani Petrosyan, Number of Data Records Exposed Worldwide From 1st Quarter 2020 to 3rd Quarter 2022, STATISTA (Aug. 20, 2024), https://www.statista.com/statistics/1307426/number-of-databreaches-worldwide, last visited on November 25, 2024 .

39. When a victim's data is compromised in a breach, the victim is exposed to serious ramifications regardless of the sensitivity of the data—including but not limited to identity theft, fraud, decline in credit, inability to access healthcare, as well as legal consequences.[12]

40. The U.S. Department of Justice's Bureau of Statistics has found that "among victims who had personal information used for fraudulent purposes, 29 percent spent a month or more resolving problems" and that resolution of those problems could take more than a year.[13]

41. The U.S. Government Accountability Office ("GAO") has concluded that it is common for data thieves to hold onto stolen data for extended periods of time before utilizing it for identity theft.[14]

42. In the same report, the GAO noted that while credit monitoring services can assist with detecting fraud, those services do not stop it.[15]

[12] 2017 Annual Data Breach Year-End Review, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/wpcontent/uploads/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf.

[13] Victims of Identity Theft, 2014, U.S. DEPARTMENT OF JUSTICE, BUREAU OF JUSTICE STATISTICS (Nov. 13, 2017) https://bjs.ojp.gov/content/pub/pdf/vit14.pdf, last visited on November 25, 2024.

[14] Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services, U.S. GOV'T ACCOUNTABILITY OFF., https://www.gao.gov/assets/700/697985.pdf, last visited on November 25, 2024.

[15] *Id.*

43. PII is a valuable commodity for which a black market exists on the dark web, among other places. Personal data can be worth from $1,000-$1,200 on the dark web and the legitimate data brokerage industry is valued at more than $250 billion.[16]

44. In this black market, criminals seek to sell stolen data to identity thieves who desire the data to extort and harass victims, take over victims' identities in order to open financial accounts, and otherwise engage in illegal financial transactions under the victims' names.[17]

The Sensitivity of Customers' PII Demands Heightened Protection

45. Entities in the financial industry are popular targets for cyberattacks and require top tier security measures to protect PII, especially given that these databases store sensitive patient records.

46. Countless victims impacted by the Data Breach now face a constant threat of being repeatedly harmed, including but not limited to living the rest of their lives knowing that criminals can compile, build, and amass profiles on them for decades – exposing them to a continuing threat of identity theft, disclosure of PII, threats, extortion, harassment and phishing scams, and the attendant anxiety from not knowing how one's information will be used when it comes into nefarious individuals' hands.

---

[16] Ryan Smith, *Revealed: How Much is Personal Data Worth on the Dark Web?*, INSURANCE BUSINESS MAGAZINE, https://www.insurancebusinessmag.com/ca/news/cyber/revealed--how-much-ispersonal-data-worth-on-the-dark-web-444455.aspx, last visited November 25, 2024; see also Maria LaMagna, The Sad Truth About How Much Your Google Data is Worth on the Dark Web, MARKETWATCH, https://www.marketwatch.com/story/spooked-by-the-facebook-privacy-violationsthis-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20, last visited November 25, 2024; Emily Wilson, The Worrying Trend of Children's Data Being Sold on the Dark Web, THE NEXT WEB (Feb. 23, 2019), https://thenextweb.com/news/children-data-sold-the-dark-web, last visited November 25, 2024.

[17] *How Much is Your Data Worth? The Complete Breakdown for 2024*, INVISIBLY (Jul. 13, 2021), https://www.invisibly.com/learn-blog/how-much-is-data-worth/.

47. Due to the special risks associated with individuals' data breaches and the increasing frequency with which they are occurring, it is imperative for entities like Defendant to routinely: (a) monitor for system breaches, cyberattacks and other exploitations; and (b) update their software, security procedures, and firewalls.

Data Breaches Are Preventable

48. As explained by the United States Government, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[18]

49. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.

[18] How to Protect Your Networks from Ransomware, available at https://www.justice.gov/criminal-ccips/file/872771/download (last visited November 25, 2024).

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. Ifa user only needs to read specific files, the user should not have written access to those files, directories, or shares.

- Disable macro scripts from office files transmitted Via email. Consider using Office Viewer software to open Microsoft Office files transmitted Via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[19]

50. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet—facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

---

19 *Id*.

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[20]

51. Given that Defendant was storing the sensitive PII, it could and should have implemented all of the above measures to prevent and detect cyberattacks.

52. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach

[20] See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: https://www.microsoft.com/security/blog/ZO20/03/05/human-operated-ransomware-attacks-a-preventable-disaster/, last accessed November 25, 2024.

and the exposure of the PII of at least tens of thousands of individuals, including that of Plaintiff and Class Members.

Defendant Was and Is Well Aware of the Threat of Cyber Theft and Exfiltration

53. Plaintiff and Class Members were required to entrust Defendant with highly sensitive and confidential PII. Defendant, in turn, collected that information and assured customers that they were acting to protect that PII and to prevent its disclosure.

54. Defendant could have prevented the Data Breach by assuring that the PII at issue was properly secured.

55. Defendant's overt negligence in safeguarding Plaintiff and Class Members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years. Further, as an entity engaged in the financial services, and related industry, Defendant was on notice that such companies are targets for data breach hackers and cyber-thieves.

56. Hackers prey on s financial institutions and related entities that collect and maintain sensitive information. Companies like Defendant have been aware of this, and the need to take adequate measures to secure their systems and information, for a number of years. Companies like Defendant are well aware of the risk that data breaches pose to consumers, especially because both the size of its customer base and the fact that the PII that it collects and maintains is profoundly valuable to hackers. In 2021, 1,862 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, an increase of 68% over 2020 and a 23% increase

over the previous all-time high.[21] These data breaches exposed the sensitive data of approximately 294 million people. *Id.*

57. It can be inferred from the Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiff and Class Members' PII.

58. Upon information and belief, prior to the Data Breach, Defendant was aware of its security failures, but failed to correct them or to disclose them to the public, including Plaintiff and Class Members.

59. The implementation of proper data security processes requires affirmative acts. Accordingly, Defendant knew or should have known that it did not make such actions and failed to implement adequate data security practices.

60. Because Defendant failed to comply with industry standards, while monetary relief may cure some of Plaintiff and Class Members' injuries, injunctive relief is necessary to ensure Defendant' approach to information security is adequate and appropriate. Upon information and belief, Defendant still maintains the PII of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Plaintiff's and Class Members' PII remain at risk of subsequent data breaches.

61. In addition to its obligations under state and common laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff

[21] ITRC_2021_Data_Breach_Report.pdf, available at https://www.idtheftcenter.org/wp-content/uploads/2022/04/ITRC_2021_Data_Breach_Report.pdf , last visited November 25, 2024.

and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Plaintiff and Class Members.

62. Defendant owed a duty to Plaintiff and Class Members to ensure that the PII it collected and was responsible for was adequately secured and protected.

63. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII and financial information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

64. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach that impacted the PII it collected and was responsible for in a timely manner.

65. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

66. Defendant owed a duty to Plaintiff and Class Members to disclose if its data security practices was inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

67. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

68. Defendant owed a duty to Plaintiff and Class Members to mitigate the harm suffered by the Representative Plaintiff and Class Members as a result of the Data Breach.

69. Defendant retain and store this PII and derive a substantial economic benefit from said PII.

70. Plaintiff and Class Members provided their PII with the reasonable expectation and mutual understanding that recipient Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

71. Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members, who value the confidentiality of their PII and demand security to safeguard their PII, took reasonable steps to maintain the confidentiality of their PII.

72. Defendant derived a substantial economic benefit from collecting Plaintiff and Class Members' PII. In addition to obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' PII, Defendant assumed legal and equitable duties, and knew or should have known it was responsible for protecting Plaintiff and Class Members' PII from disclosure.

73. At all times material, Defendant were under a duty to adopt and implement reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant also had a legal duty created by contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

74. Defendant, via its Privacy Policy, either directly or indirectly promised and assumed a duty to maintain and protect the PII of Plaintiff and the Class, demonstrating an understanding of the importance of securing PII.

75. Defendant's failure to safeguard the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

76. Defendant was not permitted to disclose Plaintiff and Class Members' PII for any reason that would apply in this situation. The disclosure of Plaintiff and Class Members' PII via the Data Breach was not permitted per Defendant's own policies.

77. Defendant failed to use reasonable security procedures and practices appropriate to safeguard the sensitive, unencrypted information it was maintaining of Plaintiff and Class Members, consequently enabling and causing the exposure of PII in the Data Breach.

Defendant Violated FTC Guidelines Prohibiting Unfair or Deceptive Acts

78. The Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") prohibits businesses from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See e.g., FTC v. Wyndham Corp.*, 799 F.3d 236 (3d Cir. 2015).

79. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[22]

80. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[23]

[22] See https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited November 25, 2024).

[23] See https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited November 25, 2024).

81. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

82. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

83. Defendant failed to properly implement basic data security practices. Defendant' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

84. In that regard, Defendant was at all times fully aware of its obligations to protect Plaintiff and Class Members' PII because of their business model of collecting PII and storing such information. Defendant was also aware of the significant repercussions that would result from their failure to do so.

85. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that they and any of their affiliates would comply with their obligations to keep such information confidential and secure from unauthorized access.

86. Had Defendant disclosed to Plaintiff and Class Members that its data systems were not secure and were vulnerable, Plaintiff would not have entrusted such entities with such sensitive

information. In fact, Defendant would have been forced to adopt reasonable data security measures and to comply with state and federal law.

87. Defendant knew or should have known that Plaintiff and Class Members would reasonably rely upon, and trust Defendant' express and implied promises regarding the security and safety of its data and systems.

88. By collecting victims' sensitive PII and failing to protect it by maintaining inadequate security systems, failing to properly archive the PII, allowing access of third parties, and failing to implement security measures, Defendant caused harm to Plaintiff and all affected individuals.

The Impact of the Data Breach on Plaintiff and the Class

89. As explained above, exposure of PII to the wrong people can have profound consequences. The impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives.

90. Identity theft can impact an individual's ability to get credit cards and obtain loans, such as student loans or mortgages.[24] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

91. The U.S. GAO found that, "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[25]

---

[24] Identity Theft: The Aftermath 2017, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf, last visited November 25, 2024.

[25] Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, U.S. GOV'T ACCOUNTABILITY OFF. (June 2007), https://www.gao.gov/new.items/d07737.pdf, last visited November 25, 2024.

92. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches:

> *"[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."*[26]

93. Defendant was also aware of the significant repercussions that would result from its failure to protect PII and knew, or should have known, the importance of safeguarding the PII entrusted to themselves and of the foreseeable consequences in the event of a breach of its data security. Nonetheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

94. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen. As a result, victims suffer both immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

95. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. They must now be vigilant and continuously review their credit reports for suspected incidents of identity theft, educate themselves about security freezes, fraud

[26] Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, U.S. GOV'T ACCOUNTABILITY OFF. (June 2007), https://www.gao.gov/new.items/d07737.pdf, last visited November 25, 2024.

alerts, and take steps to protect themselves against identity theft, which will extend indefinitely into the future.

96. Even absent any adverse use, consumers suffer injury from the simple fact that PII has been stolen. When such sensitive information is stolen, accounts become less secure, and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the community.

97. Plaintiff and the other Class Members also suffer ascertainable losses in the form of opportunity costs and the time and costs reasonably incurred to remedy or mitigate the effects of the Data Breach, including:

A. Monitoring compromised accounts for fraudulent charges;

B. Purchasing credit monitoring and identity theft prevention;

C. Taking trips to banks and waiting in line to verify their identities in order to restore access to compromised accounts;

D. Placing freezes and alerts with credit reporting agencies;

E. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

F. Contacting their financial institutions and closing or modifying financial accounts;

G. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

H. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled; and,

I. Closely reviewing and monitoring financial accounts and credit reports for unauthorized activity for years to come.

98. Moreover, Plaintiff and the other Class Members have an interest in ensuring that Defendant implements reasonable security measures and safeguards to maintain the integrity and confidentiality of the PII, including making sure that the storage of data or documents containing PII is not accessible by unauthorized persons, that access to such data is sufficiently protected, and that the PII remaining in the possession of Defendant is fully secure, remains secure, and is not subject to future theft.

99. As a further direct and proximate result of Defendant's actions and inactions, Plaintiff and the other Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

100. As a direct and proximate result of Defendant's wrongful actions or omissions here, resulting in the Data Breach and the unauthorized release and disclosure of Plaintiff and other Class Members' PII, Plaintiff and all Class Members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) the resulting increased and imminent risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other personal accounts—for which they are entitled to compensation; and (iii) emotional distress as a result of having their PII accessed and exfiltrated in the Data Breach.

101. But for Defendant' unlawful conduct, scammers would not have access to Plaintiff and Class Members' PII. Defendant' unlawful conduct has directly and proximately resulted in a widespread threat of digital attacks against Plaintiff and Class Members.

102. Breach victims have spent significant time monitoring personal accounts (banking, credit monitoring, financial applications, and even other applications/accounts that may be attacked) for fraudulent activity. Many breach victims have had to change their passwords and associated accounts which may be connected to various pieces of stolen PII. Plaintiff have been monitoring their credit activity, living in constant fear and apprehension of further attacks.

103. Phishing and other targeted attacks result from data breaches that disclose PII. Phishing scammers use emails and text messages to trick people into giving them their personal information, including but not limited to passwords, account numbers, and social security numbers. Phishing scams are frequently successful, and the FBI reported that Americans lost approximately $57 million to such scams in 2019 alone.[27]

104. Given the sensitive nature of the information stolen, and its dissemination to unauthorized parties, Plaintiff has already suffered injury and remain at a substantial and imminent risk of future harm.

105. Plaintiff and Class Members are now forced to research and subsequently acquire credit monitoring and reasonable identity theft defensive services and maintain these services to avoid further impact. Plaintiff anticipates substantial out-of-pocket expenses to pay for these services.

[27] *How to Recognize and Avoid Phishing Scams*, FEDERAL TRADE COMMISSION (Sept. 2022), https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

106. In sum, Plaintiff and similarly situated consumers have been injured as follows due to the Data Breach:

a. Theft of their PII and the resulting loss of privacy rights in that information;

b. Improper disclosure of their PII;

c. Loss of value of their PII;

d. The amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures;

e. Defendant's retention of profits attributable to Plaintiff and other Class Members' PII that Defendant failed to adequately protect;

f. Economic and non-economic impacts that flow from imminent, and ongoing threat of fraud and identity theft to which Plaintiff and Class Members are now exposed to;

g. Ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of this Data Breach;

h. Emotional distress, and fear associated with the imminent threat of harm from the continued phishing scams and attacks as a result of this Data Breach.

The Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

107. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of PII involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes —e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

108. Such fraud may go undetected until debt collection efforts commence months, or even years, later. An individual may not know that their PII was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected triggering potential unpleasant interaction with the IRS.

109. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

110. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant' Data Breach.

Defendant' Delayed Notification of the Breach

111. Time is of the essence when highly sensitive PII is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII of Plaintiff and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII, and face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing critical PII and/or PHI.

112. Despite this knowledge and understanding, Defendant did not timely inform affected individuals, including Plaintiff and Class Members, about the Data Breach, waiting until November 2024 – approximately almost 5 full months after it detected suspicious activity in May 2024 – to provide notice.

113. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.6% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[28]

114. According to the U.S. Bureau of Labor Statistics' 2022 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week; leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[29, 30] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

115. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

V. CLASS ALLEGATIONS

116. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiff asserts common law claims on behalf of themselves and all Class Members for negligence (Count I), breach of implied contract (Count II), and breach of fiduciary duty (Count III), on behalf of the

[28] U.S. BUREAU OF LABOR STATISTICS, Wage Worker Survey, available at https://www.bls.gov/opub/reports/minimum-wage/2022/home.htm (last visited November 25, 2024); see also U.S. BUREAU OF LABOR STATISTICS, Employment And Average Hourly Earnings By Industry, available at https://www.bls.gov/news.release/empsit.t19.htm (last visited November 25, 2024) (finding that on average, private-sector workers make $1,216.28 per 40-hour work week).

[29] See https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html?&qsearchterm=James%20Wallman (last visited November 25, 2024).

[30] *Id.*

Nationwide Class defined below, and in the alternative, brings Counts I-III on behalf of a Michigan state sub-class, as defined below.

Nationwide Class: All residents of the United States whose PII was accessed or otherwise compromised as a result of the Data Breach.

Michigan Sub-Class: all residents of the State of Michigan whose PII was accessed or otherwise compromised as a result of the Data Breach.

Members of the Nationwide Class and the Michigan Sub-Class, are referred to herein collectively as "Class Members" or the "Class."

117. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

118. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

119. **Numerosity**: The exact number of members of the Class is unknown to Plaintiff at this time but, upon information and belief the number of "persons affected" by the Data Breach is approximately 1.5 million, indicating that there are numbers – over a millions – members of the Nationwide Class, making joinder of each individual impracticable. There are numerous members of the Michigan Class, making joinder of each individual impracticable. Ultimately, members of the Class will be easily identified through Defendant's records.

120. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions

predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

b) Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

c) Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members, respectively, to unauthorized third parties;

d) Whether Defendant had a duty not to use the PII of Plaintiff and Class Members for non-business purposes;

e) Whether and when Defendant learned of the Data Breach;

f) Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g) Whether Defendant committed violations by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h) Whether Defendant failed to implement and maintain reasonable security procedures and practices adequate to protect the information compromised in the Data Breach, considering its nature and scope;

i) Whether Defendant has adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j) Whether Defendant engaged in unfair, unlawful, or deceptive practices, including by failing to safeguard the PII of Plaintiff and Class Members;

k) Whether Plaintiff and Class Members are entitled to actual, consequential, and/or

nominal damages as a result of Defendant's wrongful conduct, and if so, in what amount;

l) Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct, and if so, in what amount; and

m) Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

121. **Typicality**: Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and the Class Members sustained damages as a result of Defendant's uniform wrongful conduct during transactions with them.

122. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and have retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and their counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class, and have the financial resources to do so. Neither Plaintiff nor their counsel have any interest adverse to those of the other members of the Class.

123. **Risks of Prosecuting Separate Actions**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Class. Furthermore, Defendant still collects and maintains the PII of Plaintiff, the Class and other consumers in the course of its business and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the PII entrusted to Defendant.

124. **Policies Generally Applicable to the Class**: This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Plaintiff and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant' practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff challenge to those practices hinges on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

125. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if Class Members could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

126. **Manageability**: Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

127. The Class may be certified pursuant to Rule 23(b)(2) because Defendant has acted on grounds generally applicable to the Class, thereby making final injunctive relief and corresponding declaratory relief appropriate with respect to the claims raised by the Class.

128. The Class may also be certified pursuant to Rule 23(b)(3) because questions of law and fact common to the Class will predominate over questions affecting individual members, and a class action is superior to other methods for fairly and efficiently adjudicating the controversy and causes of action described in this Complaint.

129. Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

VI. CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff, the Nationwide Class, and the Michigan Sub-Class)

130. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 129.

131. As a condition of receiving financial services from Defendant, its current and former customers were obligated to provide and entrust Defendant with certain PII, including their name, Social Security number, and other PII and financial information.

132. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

133. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed or obtained

by unauthorized parties.

134. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of its current and former customers' PII involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

135. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff and Class Members' information in Defendant's possession was adequately secured and protected.

136. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

137. Defendant had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff and the Class's PII, and to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

138. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a mandatory step in obtaining services from Defendant.

139. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Class, to maintain adequate data security.

140. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security

practices.

141. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendant's systems.

142. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's wrongful conduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiff and the Class's PII, including basic encryption techniques available to Defendant.

143. Plaintiff and the Class had no ability to protect their PII that was in, and remains in, Defendant's possession.

144. Defendant was in a position to effectively protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

145. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

146. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully accessed by unauthorized third persons as a result of the Data Breach.

147. Defendant, through its actions and inaction, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in

protecting and safeguarding the PII of Plaintiff and the Class when the PII was within Defendant's possession or control.

148. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

149. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its current and former customers' PII in the face of increased risk of theft.

150. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former customers' PII.

151. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove former customers' PII it was no longer required to retain pursuant to regulations.

152. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

153. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

154. There is a close causal connection between (a) Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and (b) the harm or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and the Class PII was accessed and exfiltrated as the direct and proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

155. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting

commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of businesses, such as Defendant, of failing to implement reasonable measures to protect PII. The FTC Act and related authorities form part of the basis of Defendant's duty in this regard.

156. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the damages that would result to Plaintiff and the Class.

157. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

158. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

159. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

160. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and

other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the current and former customers' PII in its continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

161. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

162. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

163. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff is now at an increased risk of identity theft or fraud.

164. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff is entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff, the Nationwide Class, and the Michigan Sub-Class)

165. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained above.

166. Defendant acquired and maintained the PII of Plaintiff and the Class, including their names, Social Security numbers, and other PII and financial information.

167. At the time Defendant acquired the PII of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

168. Plaintiff and the Class would not have entrusted their PII to Defendant had they known that Defendant would make the PII internet-accessible, not encrypt sensitive data elements such as Social Security numbers, and not delete the PII that Defendant no longer had a reasonable need to maintain.

169. Prior to the Data Breach, Defendant published the Privacy Notice, agreeing to protect and keep private financial information of Plaintiff and the Class.

170. Defendant further promised to protect Plaintiff's and Class Members' PII through the use of computer safeguards and secured files and buildings.

171. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class

Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

172. In collecting and maintaining the PII of Plaintiff and the Class and publishing the Privacy Notice, Defendant entered into contracts with Plaintiff and the Class requiring Defendant to protect and keep secure the PII of Plaintiff and the Class.

173. Plaintiff and the Class fully performed their obligations under the contracts with Defendant.

174. Defendant breached the contracts they made with Plaintiff and the Class by failing to protect and keep private financial information of Plaintiff and the Class, including failing to (i) encrypt or tokenize the sensitive PII of Plaintiff and the Class, (ii) delete such PII that Defendant no longer had reason to maintain, (iii) eliminate the potential accessibility of the PII from the internet where such accessibility was not justified, and (iv) otherwise review and improve the security of the network system that contained such PII.

175. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; additional time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, credit freezes, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

176. As a direct and proximate result of Defendant's breach of contract, Plaintiff are at an increased risk of identity theft or fraud.

177. As a direct and proximate result of Defendant's breach of contract, Plaintiff is entitled to and demands actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiff, the Nationwide Class, and the Michigan Sub-Class)

178. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the paragraphs above.

179. A relationship existed between Plaintiff and the Class and Defendant in which Plaintiff and the Class put their trust in Defendant to protect the PII of Plaintiff and the Class. Defendant accepted that trust and the concomitant obligations.

180. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and not disclose their PII to unauthorized third parties.

181. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

182. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of its current and former customers' PII involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

183. Defendant's fiduciary duty required it to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or

disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and the Class's information in Defendant's possession was adequately secured and protected.

184. Defendant also had a fiduciary duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's 'and the Class's PII. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant, and because Defendant was the only party in a position to know of its inadequate security measures and capable of taking steps to prevent the Data Breach.

185. Defendant breached the fiduciary duty that it owed to Plaintiff and the Class by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the PII of Plaintiff and the Class.

186. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiff and the Class.

187. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and the Class would not have occurred.

188. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and the Class.

189. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff is entitled to and demands actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

COUNT IV

Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
815 ICLS 505/1, *et seq.*
(On Behalf of Plaintiff and the Class)

190. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained above.

191. This claim is brought under the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA").

192. Plaintiff and Class Members are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e).

193. Plaintiff, the Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

194. The ICFA applies to Defendant because Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f).

195. Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

196. Defendant violated ICFA by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq., which was a direct and proximate cause of the Data Breach;

d. omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Class Members' PII; and

e. omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

197. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their PII.

198. Defendant intended to mislead Plaintiff and Class Members and induce them to rely on their omissions.

199. Had Defendant disclosed to Plaintiff and Class Members (or their third-party agents) that their data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the PII that Plaintiff and Class Members (or their third-party agents) entrusted to them while keeping the inadequate state of their security controls secret from the public. Accordingly, Plaintiff and Class Members acted

reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

200. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff's and Class Members' rights.

201. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

202. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

203. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law.

204. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class. Plaintiff and the Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

205. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff and the Class of the nature and extent of the Data Breach pursuant to the Illinois PII Protection Act, 815 ILCS 530/1, *et seq.*

206. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of

Defendant's violations of the ICFA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and all Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class as defined herein, and appointing Plaintiff and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff' and the Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and the Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personally identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personally identifying information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining Plaintiff' and Class Members' personally identifying information on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other areas of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks; xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all

employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personally identifying information, as well as protecting the personally identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personally identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to adequately educate all Class Members about the threats that they face as a result of the loss of their confidential personally identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs

sufficient to track traffic to and from Defendant's servers; and, for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to Class Counsel, and to report any material deficiencies or noncompliance with the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of reasonable attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

VII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: November 26, 2024

Respectfully Submitted,

/s/ *Gary M. Klinger*
Gary M. Klinger (IL Bar No. 6303726)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

BARRACK, RODOS & BACINE
STEPHEN R. BASSER*
SAMUEL M. WARD*
600 West Broadway, Suite 900
San Diego, CA 92101
sbasser@barrack.com
sward@barrack.com
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

BARRACK, RODOS & BACINE
ANDREW J. HEO*
Two Commerce Square
2001 Market Street, Suite 3300
Philadelphia, PA 19103
aheo@barrack.com
Telephone: (215) 963-0600
Facsimile: (215) 963-0838

Attorneys for Plaintiff and
The Proposed Class

**Pro Hac Vice Forthcoming*